Key Recovery Policy
for the
United States Department of Defense

Version 3.0

August 31, 2003

Prepared by:

DoD Public Key Infrastructure Program Management Office

Approved:

John P Stenbit

Assistant Secretary of Defense
(Networks and Information Integration)

This page intentionally left blank.

TABLE OF CONTENTS

1 INTRODUCTION

As part of the United States Department of Defense (DoD) Key Management Infrastructure (KMI), DoD is developing a public key infrastructure (PKI). The PKI manages the registration, issuance and control of X.509 certificates for use by DoD personnel in the conduct of official business. An X.509 certificate binds an end entity (such as a subscriber, router, or automated message guard) to a key pair, certifying that the entity identified in the certificate has the private key associated with the public key incorporated into the certificate. The key pairs are used by end entities to perform cryptographic operations: to digitally sign information, to ensure the identity of the signer and the integrity of the information, and to encrypt information to ensure confidentiality. The DoD PKI issues separate certificates and key pairs for identity authentication and integrity, and for confidentiality.

This Key Recovery Policy (KRP) applies only to the encryption certificate key pair, since the DoD X.509 Certificate Policy (CP) states that "under no circumstances shall a key used to support non-repudiation services be held in trust by a third party."

The public key of the encryption certificate key pair is publicly available. The private key associated with the encryption certificate is only in the possession of the individual to whom it is issued unless other measures are taken. DoD requires a system to ensure that private keys associated with encryption certificates, which are necessary for the recovery of encrypted data, be available, as required to facilitate the proper functioning of the Department.

DoD has chosen to implement this requirement via a key escrow system. The key stored in this key escrow system, any part of the key, or information necessary to access the extracted key are referred to by this policy as the "escrowed key". This policy delineates how escrowed key is stored, how authorized personnel can submit requests for copies of the escrowed key, how it is retrieved, and how it is delivered to an authorized requestor. It also specifies how escrowed key is protected during each of these activities.

This part of the DoD PKI supports data recovery for business, law enforcement and counterintelligence requirements; however, it does not provide a data recovery service. In addition, this policy is not intended to change the authority of any individual or organization to access data. It provides the mechanism for obtaining a copy of the escrowed key where access to that key is a necessary condition for access to data.

1.1 OVERVIEW

This policy is for use by DoD Class 3 and Class 4 PKIs that escrow keys. It includes requirements that apply to personnel who: are subscribers of the PKI, request escrowed keys, or participate in the process of extracting and delivering the escrowed key to the requestor.

1.2 IDENTIFICATION

N/A

1.3 COMMUNITY AND APPLICABILITY

1.3.1 Key Escrow System Roles

- Key Recovery Agent (KRA)
- Key Recovery Official (KRO)
- Requestor
- Subscriber

A KRA is an individual who, using a two party control procedure with a second KRA, is authorized, as specified in the applicable Key Recovery Practice Statement (KRPS) (see Glossary, Section 0), to interact with the key escrow database in order to extract an escrowed key.[1]

A KRO is a local individual who receives requests for escrowed keys, verifies the requestor's identity and authorization and transmits that information to a KRA who can perform the requested extraction of the escrowed key.

A requestor is an individual who requests an escrowed key and to whom the extracted key is to be delivered.

A subscriber is the person or device that is the original holder of the private key.

1.3.2 Key Escrow System Components

A key escrow system consists of the following components:

[1] For the Class 4 FORTEZZA/Network Security Manager (NSM) PKI, the requirement for two party control procedure is satisfied by identifying the CAW operator and the ISSO as the two KRAs.

- The key escrow database, where the escrowed keys are stored,
- KRA workstations, which KRAs use to extract escrowed key from the key escrow database under two party control and
- Equipment used by the KRO to facilitate protected delivery of copies of escrowed keys to the requestor.

1.4 CONTACT DETAILS

1.4.1 KRA Policy Administration Organization

This Policy shall be administered by the DoD PKI Program Management Office (PMO).

1.4.2 Contact Person

The contact person is:

DoD PKI PMO
ATTN: V
DEPARTMENT OF DEFENSE
9800 SAVAGE RD STE 6737
FT MEADE MD 20755-6737

1.4.3 Person Performing Policy/Practice Compatibility Analysis

The Policy Management Authority (PMA) shall determine the suitability of any KRPS to this policy.

This page intentionally left blank.

2 GENERAL PROVISIONS

2.1 OBLIGATIONS

As part of the key escrow process, subscribers are notified that the private keys associated with their encryption certificates will be escrowed.

During delivery, escrowed keys shall be protected against disclosure to any party except the requestor.

The KRPS will describe the method for ensuring that each individual understands and complies with the obligations for any Key Recovery role they execute.

2.1.1 KRA Obligations

A KRA who provides escrowed keys to requestors under the Policy defined in this document shall conform to the stipulations of this document. In particular, the following stipulations apply:

- The KRA shall maintain an approved copy of the KRPS that complies with this KRP.
- The KRA shall provide a KRPS (and any subsequent changes) to the PMA for compliance assessment, if not operating under an already-approved KRPS.
- The KRA shall operate in accordance with the stipulations of the approved KRPS.
- The KRA shall protect copies of subscribers' escrowed keys from unauthorized disclosure.
- The KRA shall release escrowed keys only for properly authenticated and authorized requests from requestors, as specified in this Policy.
- The KRA shall protect all information, including the KRA's own key(s) that could be used in the recovery of subscribers' escrowed keys.
- The KRA shall not release information (including subscriber notification) regarding key recovery requests.
- The KRA shall monitor key recovery requests for each subordinate KRO to identify potentially anomalous activities and shall initiate investigative activities as deemed appropriate.

2.1.2 KRO Obligations

A KRO who submits requests as described in this Policy shall comply with the stipulations of this Policy and comply with the applicable KRPS. In particular, the following stipulations apply:

- The KRO shall protect copies of escrowed keys from compromise.
- The KRO, as an intermediary for the KRA, shall request escrowed keys only upon receipt of a request from an authorized key recovery requestor.
- The KRO, as an intermediary for the KRA, shall request an escrowed key only for the purpose for which the request is authorized.
- The KRO shall protect all information, including the KRO's own key(s) that are used as part of the key recovery process.
- The KRO shall represent themselves accurately to all entities when requesting key recovery services.
- The KRO shall not release information (including subscriber notification) regarding key recovery requests.

2.1.3 Requestor Obligations

A requestor who initiates key recovery requests as described in this Policy shall comply with the following stipulations:

- Requestors shall protect copies of escrowed keys from compromise.
- Requestors shall request escrowed keys only to recover subscriber data they are authorized to access.
- Requestors shall use the escrowed key only to recover subscriber data they are authorized to access.
- Requestors shall represent themselves accurately to all entities during any key recovery service.
- If and when the copy of the escrowed key is no longer required for the requested purpose, the requestor shall dispose of it in accordance with the applicable KRPS.
- Requestors shall acknowledge receipt of the escrowed key and their responsibilities for use, protection, and destruction of the escrowed key.
- Unless the key recovery is for purposes that require that the subscriber not be made aware of the action, the requestor shall notify the subscriber regarding the key recovery request.

2.1.4 Subscriber Obligations

Subscribers shall comply with the following stipulations:

- Subscribers shall provide accurate identification and authentication information during initial registration and subsequent key recovery requests.

- When the subscriber is notified that his or her escrowed key has been recovered, the subscriber shall determine whether revocation of the recovered key is necessary. The subscriber shall request the revocation.

2.2 REQUIREMENTS SUPPORTING NON-U.S. GOVERNMENT SUBSCRIBERS

2.2.1 Liability

A non-US Government subscriber will have no claim against the DoD arising from use of the subscriber's certificate or a KRA's determination to provide copies of escrowed keys to an authorized key recovery requestor in response to a duly authorized request. In no event will the DoD be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any such key recovery request completed by a DoD KRA.

2.2.2 Governing law

This Policy shall be governed by the laws of the United States of America.

2.3 INTERPRETATION AND ENFORCEMENT

2.3.1 Severability of provisions, survival, merger, and notice

Should it be determined that one section of this Policy is incorrect or invalid, the other sections shall remain in effect until the Policy is updated. Requirements for updating this Policy are described in Section 7. Responsibilities, requirements, and privileges of this document are merged to the newer edition upon release of that newer edition.

2.3.2 Dispute resolution procedures imposed on Subscribers

The PMA shall decide any disputes over the interpretation or applicability of the DoD KRP.

2.4 PUBLICATION AND REPOSITORY

N/A

2.5 COMPLIANCE AUDIT

Compliance audits shall be performed as specified in the DoD X.509 CP. Audit of the key escrow database shall be performed as specified for Certification Authority (CA) audits. Audits for KRAs and KROs shall be performed as specified for Certificate Management Authorities (CMAs) subordinate to a CA.

Where precise frequencies are specified for the completion of scheduled compliance audits, it is recognized that circumstances unrelated to the compliance audit (e.g., natural disaster or armed conflict) could make it impossible to conduct a required audit within the specified time constraint. In such cases, the audited organization may request and be granted a short-term extension not to exceed 90 days.

2.6 CONFIDENTIALITY

2.6.1 Types of information to be protected

To verify a requestor's identity and authorization for escrowed keys, the KRA or KRO is authorized to request authentication or authorization evidence from the requestor that may be considered personal confidential or sensitive unclassified information. Any such information shall be explicitly identified in the KRPS. All such information stored at the KRA's or KRO's location shall be handled as sensitive and access to the information shall be restricted to those with an official need-to-know in order to perform their functions.

2.6.2 Information release circumstances

A KRA will not disclose or allow to be disclosed escrowed key or escrowed key-related information to any third party unless authorized by this Policy; required by law, government rule, or regulation; or by order of a court of competent jurisdiction. The identity of the requestor of escrowed key or escrowed key-related information shall be authenticated per Section 3, Identification and Authentication.

3 IDENTIFICATION AND AUTHENTICATION

Identification and Authentication verify that requestors are who they say they are and are authorized to access requested escrowed key.

The user's authenticated identity shall be used as the basis for determining the user's access permissions and providing user accountability.

3.1 IDENTITY AUTHENTICATION

Identity authentication shall be commensurate with the DoD PKI certificate assurance level. It shall comprise the activities specified by the DoD X.509 CP for authentication of individual identity during initial registration for at least the specified DoD PKI certificate assurance level or be based on digital signatures that can be verified using public key certificates for at least the specified DoD PKI certificate assurance level.

3.2 REQUESTOR

The requirements for authentication and authorization when the requestor is the subscriber are addressed in Section 3.3 "Subscriber".

3.2.1 Requestor Authentication

The requestor shall establish his or her identity to the KRA or the KRO, as an intermediary for the KRA, as specified in Section 3.1. The KRA or KRO shall personally verify the identity of the requestor prior to initiating the key recovery request. The authentication mechanism shall be detailed in the KRPS.

3.2.2 Requestor Authorization Verification

The KRA or the KRO, as an intermediary for the KRA, shall validate the authorization of the requestor in consultation with organization management and/or legal counsel, as appropriate. The mechanism to validate the authorization shall be detailed in the KRPS.

3.3 SUBSCRIBER

3.3.1 Subscriber Authentication

The subscriber shall establish his or her identity to the KRA or the KRO, as an intermediary for the KRA, as specified in Section 3.1. If the authentication is not based on digital signatures that can be verified using the public key certificates for at least the given DoD PKI certificate assurance level, the KRA or KRO shall personally verify the identity of the subscriber prior to initiating the key recovery request. The authentication mechanism shall be detailed in the KRPS.

For automated recovery, the subscriber must be authenticated to the key escrow system using a valid DoD public key certificate. The authentication mechanism shall be detailed in the KRPS. The assurance level of the authentication certificate shall be equal to or greater than that of the certificate associated with the escrowed key.

3.3.2 Subscriber Authorization Verification

Current subscribers are authorized to recover their own escrowed key material.

3.4 KRA AND KRO AUTHENTICATION

3.4.1 KRA

The KRA shall authenticate identity to the key escrow database using a digital signature. The DoD PKI certificate assurance level associated with the certificate shall be at least the DoD PKI certificate assurance level required to access the key escrow database.

3.4.2 KRO

The KRO shall authenticate identity to the KRA using a digital signature. The DoD PKI certificate assurance level associated with the certificate shall be at least the DoD PKI certificate assurance level required to access the key escrow database.

4 OPERATIONAL REQUIREMENTS

4.1 ESCROWED KEY RECOVERY REQUESTS

4.1.1 Who Can Request Recovery of Escrowed Keys

Subscribers may request recovery of their own escrowed keys. Key recovery may also be requested by third parties:

- ❑ Any military or DoD civilian manager, supervisor, or commander for any subordinate military, DoD civilian, or contractor subscriber,
- ❑ Law Enforcement / Counterintelligence agents,
- ❑ Agents of U.S. Federal Courts,
- ❑ Any person authorized by the subscriber to request recovery of the subscriber's escrowed key, or
- ❑ Any person or organization authorized by the DoD PMA via an authenticated communication.

4.1.2 Requirements for Requesting Escrowed Key Recovery

Subscribers may use automated means to request their escrowed keys from the Key Escrow Database if they possess a valid DoD PKI issued authentication certificate of appropriate assurance level.

Subscribers may submit requests on their own behalf directly to the KRA. If the KRPS does not allow this procedure, the subscriber must fill out a physical or electronic request, as specified in the applicable KRPS, sign it by hand or digitally, if they have a DoD PKI certificate with DoD X.509 CP assurance level greater than or equal to that of the escrowed key, and submit the request to the KRO.

Military Commanders, Supervisors, or managers must fill out a physical or electronic request, as specified in the applicable KRPS, sign it by hand or digitally, if they have a DoD PKI certificate with DoD X.509 CP assurance level greater than or equal to that of the escrowed key, and submit the request to the KRO.

If the public key certificate for the requested escrowed key asserts one or more clearances, compartments, and/or formal access approvals, the requestor must provide, and the KRO verify, evidence that the requestor possesses all clearances, compartments, and/or formal access approvals asserted in the certificate.

In all instances where the requestor is neither the subscriber nor the subscriber's Military Commander, Supervisor, or manager, the requestor must fill out a physical or electronic request, as specified in the applicable KRPS, sign it by hand or digitally, if they have a DoD PKI certificate of equivalent or higher class than the escrowed key, and submit it to the KRO.

Key recovery operations that require release of escrowed keys outside the jurisdiction of the DoD shall be bound, by legal and policy means, to the key protection and other provisions of the DoD KRP and the DoD X.509 CP.

4.2 PROTECTION OF ESCROWED KEYS

Escrowed keys shall be stored in a protected key escrow database.

Key recovery (in particular automated key recovery) must be carried out with extreme caution, as the chance for compromise can be very high. Further, the risk of compromise and the scope of any potential compromise is implementation dependent.

4.2.1 Key Recovery through the KRA

The KRA shall provide access to a copy of an escrowed key only in response to a properly authenticated and authorized key recovery request. Such access shall require the actions of at least two KRAs. All copies of escrowed keys shall be protected continuously by two person control procedures during recovery and delivery to the authenticated and authorized requestor. The protection mechanisms shall be specified in the KRPS. Split key or password procedures are considered adequate two person control.

The strength of the confidentiality provided by the delivery mechanism for copies of escrowed keys shall be equal to or greater than that provided by the key being protected.

4.2.2 Subscriber Automated Recovery

A current subscriber's escrowed keys may be provided directly to that subscriber without imposition of two person control requirements. The Key Escrow Database shall only provide escrowed keys to current subscribers without two person control upon:

- Verifying that the authenticated identity of the requestor is the same as the subscriber associated with the escrowed keys being requested. The KRPS shall describe how the identity of the authenticated subscriber is verified and ensured to be same as that associated with the subscriber private key;
- Attempt to notify the subscriber of all attempts (successful or unsuccessful) to recover the subscriber's escrowed keys that are made by entities claiming to be the subscriber. If the Key Escrow Database does not have information (e.g., an e-mail address) necessary to attempt to notify the subscriber of a key recovery request, then the Key Escrow Database shall not provide the subscriber with the requested key material using the automated recovery process;

- Ensuring that the escrowed keys are being sent only to the authenticated subscriber associated with the escrowed keys; and

- Ensuring that the escrowed keys are encrypted during transmission using cryptography of strength equal to or greater than that provided by the escrowed keys.

4.3 CERTIFICATE ISSUANCE

Certificates are issued by the CA. Neither KRAs nor KROs issue certificates.

4.4 CERTIFICATE ACCEPTANCE

N/A

4.5 SECURITY AUDIT PROCEDURES

Security auditing capabilities of the underlying key escrow database and KRA workstation equipment operating system shall be enabled during installation.

4.5.1 Types of events recorded

The key escrow database equipment shall be configured to record, at a minimum, the following event types:

- Key escrow database application access (e.g., logon/logoff);
- Messages received from any source requesting key escrow database actions, (i.e., escrowed key retrieval requests);
- Actions taken in response to requests for key escrow database actions;
- Physical access to, loading, zeroizing, transferring keys to or from, backing-up, acquiring or destroying key escrow database cryptographic modules;
- Receipt of keys for escrow and posting of these keys to the key escrow database;
- Retrieval, packaging (e.g., keying or other cryptologic manipulations), securing, and shipping copies of escrowed keys;
- Anomalies, error conditions, software integrity check failures, receipt of improper or misrouted messages; and
- Any known or suspected violations of physical security, suspected or known attempts to attack the key escrow database equipment via network attacks, equipment failures, power outages, network failures, or violations of this key recovery policy.

KRA workstation equipment shall be configured to record the following event types:

The KRA equipment shall record server installation, access, and modification (to include changes in configuration files, security profiles, administrator privileges).

The KRA shall record the following events for audit:

- KRA equipment access (e.g., room access),
- Messages received from any source requesting KRA actions, (e.g., key recovery requests, second party key recovery approval requests);
- Messages sent to any destination authorizing key recovery actions, (e.g., first party escrowed key retrieval authorizations, second party key recovery approvals);
- Access to KRA databases, and
- Any use of the KRA signing key.

The KRO shall record the following information for audit:

- Transfer of escrowed keys to requestors, if transmitted through the KRO,
- Any security-relevant actions performed in support of delivery of escrowed keys, and
- Requestor identity and authorization verification (including copies of authorizations; e.g., court orders) supporting key recovery requests acted upon by the KRO.

For each auditable event defined in this section, the key recovery security audit record shall include, at a minimum:

- the type of event
- the time the event occurred
- for messages from KRAs, KROs, or other entities requesting key escrow database actions, the message source, destination and contents
- for requested key escrow database actions – a success or failure indication
- for operator initiated actions (including equipment and application access), the identity of the equipment operator who initiated the action.

Where possible, the security audit data shall be automatically collected; when this is not possible a log book, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained in accordance with the requirements of Section 4.5.3, and made available during compliance audits.

4.5.2 Audit Log Processing

If automated audit logs are required pursuant to Section 4.5.1, the applicable audit logs shall be processed as required to prevent audit overflow, audit overwrite or stoppage of system operation.

4.5.3 Audit Log Retention Period

Audit logs shall be kept until they are moved to an appropriate archive facility. Security audit data shall be retained as archive records in accordance with Section 4.6.2.

4.5.4 Audit Log Protection

Audit logs shall be protected from unauthorized modification or unauthorized deletion. No one is authorized to modify the content of audit logs, except for appending new audit records without overwriting existing audit records.

Online audit logs may only be deleted after they have been backed up to archive media. Only authorized security auditors and system administrators are allowed to delete these logs. Before deleting any online audit log, the security auditor or systems administrator must verify that the audit log data has been successfully backed up to archive media.

No one is allowed to delete or destroy audit data recorded on archive media.

4.5.5 Audit log back up procedures

Security audit processing personnel shall use the procedures described in the KRPS to perform regular back up of the audit log.

4.5.6 Audit Log Collection System (Internal vs. External)

The security audit process shall be internal to the key escrow database and KRA workstation. Security audit processes shall be invoked at component system startup and cease only at component system shutdown. The security audit process shall run automatically without human intervention.

Should it become apparent that an automated security audit system has failed, the affected key escrow system component shall cease all operations until a security audit capability can be restored.

4.5.7 Subscriber Audit Notification

There is no requirement to notify a subscriber of an audit event.

4.5.8 Vulnerability assessments

The KRA, system administrator, and other supporting personnel shall watch for attempts to violate the integrity of the key escrow system, including the equipment, physical location, and personnel. The security audit data shall be reviewed by the security auditor regularly (at least once a week) for events such as repeated failed actions, requests for escrowed keys, attempted access of escrowed keys, unauthenticated requests, or other suspicious or unusual activity. Security auditors shall also check for continuity of the security audit data.

4.6 RECORDS ARCHIVAL

The key escrow system entities shall maintain a trusted archive of information they store and of transactions they carry out. The primary objective of the archive is to be able to reconstruct the key recovery activities, in case of dispute. Examples of disputes may include:

- Validation of the identification of the recipient of a copy of the subscriber’s escrowed key.
- Establishment of the circumstances under which the escrowed key copy was provided.

- Verification of authorization and need of requestor to obtain the escrowed key copy.

4.6.1 Types of information recorded

The following information shall be archived:

- KRP and KRPS
- Security audit data
- Escrowed keys

KRPSs shall be archived by the responsible Combatant Command, Service, or Agency (C/S/A). The KRP shall be archived by the PMA.

Security audit data shall be archived by the responsible C/S/A.

The necessary software and hardware (if appropriate) must be retained, either as operational components or, after decommissioning, as archive retrieval components, to support interpretation of the information during the entire archive retention period.

Security audit data shall be archived in accordance with applicable records management regulations.

4.6.2 Archive Retention Period

The key escrow system archive retention period shall meet the requirements specified in DoD X.509 CP Section 4.6.2 for the DoD PKI certificate assurance level supported.

Escrowed keys shall be maintained within the key escrow database for a minimum of one year after the expiration of the key. The escrowed key archive retention period shall meet the archive retention period requirements specified in the DoD X.509 CP for the DoD PKI certificate assurance level supported.

4.6.3 Archive Protection

No one shall be able to modify or delete archive data unless it has been backed up to archive media. The KRPS shall specify the roles authorized to back up archive data.

No one shall be able to delete or destroy data recorded on archive media. Transfer of medium shall not invalidate digital signatures applied to the recorded data. Release of sensitive archive information will be as described in Section 2.6.2.

Archived security audit data shall be protected as specified in Section 4.5.4. Archived escrowed keys shall be protected as specified in Section 4.2.

Archive media shall be stored in a separate, safe, secure storage facility, as described by the applicable KRPS. Prior to archive, archive records shall be labeled with the CMA's distinguished name, the date, and the classification.

4.6.4 Archive backup procedures

No stipulation.

4.6.5 Requirements for time-stamping of records

The archived record shall contain information necessary to allow the security auditor to determine when the event occurred. The time precision shall be such that the sequence of events can be determined.

4.6.6 Archive Collection System (Internal vs. External)

Archive data shall be collected in any expedient manner.

4.6.7 Procedures to obtain and verify archive information

The KRPS shall describe the procedures used to verify the accuracy of the archived information.

4.7 KRA KEY CHANGEOVER

The KRA's individual and/or role-based certificates should be changed in accordance with DoD X.509 CP Section 4.7 and the applicable CPS for the DoD PKI certificate assurance level of the associated certificates.

4.8 KEY ESCROW DATABASE COMPROMISE AND DISASTER RECOVERY

Requirements for compromise or disaster notification and recovery procedures are necessary to ensure the key escrow database remains in a secure state.

4.8.1 Key Escrow Database Compromise

In the event that the key escrow database is compromised or is suspected to be compromised, recovery procedures are required to return it to a secure state. If a compromise of the key escrow database is suspected, the PMA shall be notified. The PMA shall determine the extent of the compromise and direct the appropriate action.

4.8.2 Disaster Recovery

The key escrow database shall reestablish a secure environment. The procedures for reestablishing the secure environment after any disaster must be detailed in the KRPS.

4.8.3 KRA Key Compromise

If the KRA's certificate is revoked due to compromise, there is a potential for some subscriber escrowed keys to have been exposed during the recovery process. Security auditor or system administrator personnel shall review the audit records to identify all potentially exposed escrowed keys. Each of the potentially exposed escrowed keys shall be revoked, according to procedures specified in DoD X.509 CP Section 4.4.1, and the subscriber notified of the revocation.

4.8.4 KRA Key Revocation

If the KRA's certificate is revoked for any reason, but the KRA remains authorized to perform his or her duties, then the KRA shall request a new KRA key pair from the appropriate CA. The CA shall report the old KRA key as revoked using the CA's revocation notification policy. The CA shall follow its policy for certificate issuance for the new KRA public key certificate.

4.9 KRA TERMINATION

Upon KRA termination, the DoD PMA shall take possession of all KRA archive records. The KRPS shall document the process for transferring KRA archive records to the PMA.

This page intentionally left blank.

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS

The key escrow database shall consist of equipment dedicated to the key recovery function and, optionally, CA functions.

Physical controls for the key escrow database shall be equivalent to those specified in DoD X.509 CP Section 5.1 for CA and CMA equipment. Physical controls for KRA workstations shall be equivalent to those specified in DoD X.509 CP Section 5.1 for Registration Authority (RA) and CMA equipment.

Key escrow database and KRA workstation physical controls shall be described in the KRPS.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted roles

The primary trusted roles defined by this Policy are the KRA and the KRO. (See DoD X.509 CP Section 5.2.1 for details on what constitutes a trusted role.)

5.2.1.1 Key Recovery Agent

All KRAs that operate under this Policy are subject to the stipulations of this Policy and of the PMA-approved KRPS under which it operates. The KRA's role and the corresponding procedures shall be defined in the KRPS. A KRA’s responsibilities are to ensure that the following functions occur according to the stipulations of this Policy:

- KRO functions as described in Section 5.2.1.2, if no separate KRO is employed;
- Enable (i.e., initiate or approve) the recovery of copies of escrowed keys; and
- Distribute copies of escrowed keys to requestors, with protection as described in Section 4.2;

5.2.1.2 Key Recovery Official

All KROs that operate under this Policy are subject to the stipulations of this Policy and of the PMA-approved KRPS under which it operates. The KRO’s role and corresponding procedures shall be defined in the KRPS. A KRO's responsibilities are to ensure that the following functions occur according to the stipulations of this Policy:

- Verify requestor identity and authorization as stated by this Policy;
- Build key recovery requests on behalf of authorized requestors;
- Securely communicate key recovery requests to and responses from the KRA; and
- Participate in distribution of escrowed keys to the requestor, as described by the KRPS.

The KRO role is highly dependent on public key infrastructure implementations and local requirements. The responsibilities and controls for KROs shall be explicitly described in the KRPS.

5.2.1.3 Other Trusted Roles

For Class 3 and Class 4 assurance infrastructures the KRPS shall define trusted facility roles (e.g., system administrators, security officers, operators, compliance auditors) to which shall be allocated responsibilities that ensure the proper, safe, and secure operation of the key escrow database equipment and procedures. The responsible persons who are identified in these trusted roles must be named and made available during compliance audits. The responsibilities include:

- initial configuration of the system, including installation of applications, initial setup of new accounts, configuration of initial host and network interface;
- performance of compliance audit;
- creation of devices to support recovery from catastrophic system loss;
- performance of system backups, software upgrades and system recovery;
- perform secure storage and distribution of the backups and upgrades to an off-site location;
- change of the host or network interface configuration;
- assignment of security privileges and access controls to key escrow system personnel;
- archival of the security audit log and other data as described in Sections 4.3 and 4.6 of this document;
- review of the security audit log.

5.2.2 Separation of Roles

Under no circumstances shall a KRO perform trusted facility responsibilities for a key escrow database facility. Under no circumstances shall a KRA or KRO perform their own compliance or security auditor function. Where separation among roles can be established,[2] a KRA shall not perform trusted facility responsibilities for a key escrow database facility.

Separation of responsibilities among trusted facility roles shall be described in the KRPS.

5.3 PERSONNEL CONTROLS

5.3.1 Background, qualifications, experience, and clearance requirements

Persons selected for KRA or trusted facility roles shall meet the requirements specified in DoD X.509 CP Section 5.3.1 for CMA roles. Persons selected for the KRO role shall meet the requirements specified in DoD X.509 CP Section 5.3.1 for trusted roles other than CMAs.

5.3.2 Background check procedures

Background check procedures shall be as specified in the DoD X.509 CP.

5.3.3 Training requirements

All personnel involved in key escrow database operation shall be appropriately trained. Topics shall include:

- operation of the key escrow database software and hardware,
- operational and security procedures,
- stipulations of this Policy, and
- local guidance.

The specific training required will depend on the equipment used and the personnel selected. A training plan shall be established for key escrow database installation. Training completed by the personnel shall be documented.

5.3.4 Retraining frequency and requirements

- Significant changes to key escrow database operation shall require implementation of a training (awareness) plan that includes any retraining required for KRA or KRO personnel. The execution of such plan shall be documented.

[2] For the Class 4 FORTEZZA/NSM PKI, such separation cannot be established, since the ISSO role subsumes the KRA role.

5.3.5 Job rotation frequency and sequence

Job rotation frequency and sequence shall be as specified in the DoD X.509 CP.

5.3.6 Sanctions for unauthorized actions

Appropriate administrative and disciplinary actions shall commence against personnel who violate this Policy.

5.3.7 Contracting personnel requirements

Contractor personnel requirements shall be as specified in the DoD X.509 CP.

5.3.8 Documentation supplied to personnel

Documentation requirements shall be as specified in the DoD X.509 CP.

6 TECHNICAL SECURITY CONTROLS

6.1 PROTOCOL SECURITY

When recovered by the KRAs, all copies of escrowed keys shall be protected continuously by two person control procedures during recovery and delivery to the authenticated and authorized requestor. Furthermore, the delivery mechanism for copies of escrowed keys shall provide protection against disclosure with assurance equal to or greater than the DoD PKI certificate assurance level of the certificates associated with the escrowed keys.

When a subscriber uses automated recovery, the subscriber's own escrowed keys may be provided directly to the subscriber through authenticated and encrypted channels without imposition of two person control requirements. The authentication and encryption shall be done using cryptographic means that are of strength equal to or greater than that provided by the keys being recovered. All public key certificates involved in authentication and/or encryption shall be issued by the DoD PKI and shall have an assurance level equal to or greater than that of the certificates associated with escrowed keys.

6.1.1 Key Escrow Database Protocol Security

Communications between the key escrow database and KRAs or between the key escrow database and subscribers shall be secure from protocol threats such as disclosure, modification, replay, and substitution on transactions between the key escrow database and communicating entities. The strength of all cryptographic protocols shall be equal to or greater than that of the keys they protect.

6.1.2 KRA - KRO Protocol Security

Communications between the KRA and KRO shall be secure from protocol threats such as disclosure, modification, replay, and substitution. The strength of all cryptographic protocols shall be equal to or greater than that of the keys they protect.

6.1.3 Escrowed Key Distribution Security

Communication of distributed copies of escrowed keys between the key escrow database and requestor shall be secure from protocol threats such as disclosure, modification, replay, and substitution. The strength of all cryptographic protocols shall be equal to or greater than that of the keys they protect.

6.2 KRA AND KRO PRIVATE KEYAND STORAGE KEY PROTECTION

6.2.1 Standards for Cryptographic Modules

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [Federal Information Processing Standard (FIPS) 140-1 or FIPS 140-2, as appropriate]. The PMA may determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published by the PMA. Cryptographic modules shall be validated to the FIPS 140-1 or FIPS 140-2 (as appropriate) level identified in this section, or validated, certified, or verified via one of the standards published by the PMA.

For both Class 3 and Class 4, the key escrow database, KRA workstation and KRO shall use hardware cryptographic modules that meet at least the criteria specified for FIPS 140-1 or FIPS 140-2 Level 2.

6.2.2 Private and Storage Key Control

The private components of KRA and KRO signature key pairs and encryption key pairs shall be under single person control. The key escrow database storage key shall be under two person control. The names of the individuals used for two person control shall be maintained on a list that shall be made available for compliance audits.

Storage procedures and mechanisms for the hardware cryptographic module associated with the key escrow database encryption key pair shall require two-person control. When not in use, the cryptographic module shall be stored in a secured container, such as a safe, in a facility that meets the physical security requirements of Section 5.1 of this policy.

6.2.3 Storage Key Backup

The storage key shall be backed up as necessary to provide secure continuity of key recovery operations. The backup storage key shall only be created, stored, and restored under two party control. The process of restoring the backup storage key shall maintain two party control throughout, as required in Section 6.2.2.

6.2.4 Private Key Generation and Transport

Private components of key escrow database, KRA, and KRO encryption key pairs are to be generated by and in a cryptographic module. In the event that the private component of a key escrow database, KRA, or KRO encryption key pair is to be transported from one cryptographic module to another, it must be encrypted during transport. The assurance level of the transport encryption shall be commensurate with the DoD PKI certificate Class assurance level of the key escrow database.

6.2.5 Method of Activating Private Key

Activation of private keys shall be in accordance with DoD X.509 CP section 6.2.7.

6.2.6 Method of Deactivating Private Key

The private component of the key escrow database, KRA, or KRO encryption key pair shall be deactivated as specified by the DoD X.509 CP.

6.2.7 Method of Deactivating Storage Key

Activated cryptographic modules used for key escrow database operations shall not be left unattended or otherwise open to unauthorized access. After use, they must be deactivated (e.g. via a manual logout procedure or by a passive timeout).

Hardware cryptographic modules shall be removed from operational systems and stored when not in use. If a cryptographic module contains a complete (versus split) storage key, all storage procedures and mechanisms for that module shall require two-person control.

6.3 PRIVATE KEY ACTIVATION DATA

Generation, change, and management of private key activation data shall be in accordance with DoD X.509 CP Section 6.4.

6.4 COMPUTER SECURITY CONTROLS

6.4.1 Key Escrow Database

The key escrow database used for Class 3 assurance infrastructures shall be based on trusted operating systems that are designed, implemented, and operated using the following security features:

- Individual identification and authentication,
- Secure audit,
- Residual information protection,
- Discretionary access controls,
- Operating system self-protection,

- Process isolation, and
- Meet Common Criteria (CC) Evaluation Assurance Level (EAL) 3 assurance requirements. The PMA may determine that other comparable validation, certification, or verification standards are sufficient.

The key escrow database used for Class 4 assurance infrastructures shall be hosted on operating systems that implement the requirements of Class 3, plus:

- Trusted path and
- Meet CC EAL 4 assurance requirements. The PMA may determine that other comparable validation, certification, or verification standards are sufficient.

When key escrow databases are hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system that received the evaluation rating.

Both Class 3 and Class 4 key escrow databases shall be configured to run with the minimal number of accounts and network services required to operate them. Only the required network services and ports shall be enabled, all other network services and ports shall be disabled. The key escrow databases shall be dedicated to running key recovery related or other PKI-related applications.

6.4.2 KRA Workstation

KRA workstation equipment used for Class 3 assurance infrastructures shall use operating systems that:

- Require authenticated logins,
- Provide discretionary access control, and
- Provide a security audit capability.

KRA workstation equipment used for Class 4 assurance infrastructures shall be hosted on operating systems that implement the requirements of Class 3, plus:

- Trusted path and
- Meet Common Criteria EAL 3 assurance requirements. The PMA may determine that other comparable validation, certification, or verification standards are sufficient.

When KRA workstation equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as received the evaluation rating.

Reasonable care shall be taken to prevent malicious software from being loaded on KRA workstation equipment. Only applications required to perform the organization's mission shall be loaded on the KRA workstation computer, and all such software shall be obtained from sources authorized by local policy. Data on KRA workstation equipment shall be scanned for malicious code on first use and periodically afterward.

6.4.3 KRO Equipment

Reasonable care shall be taken to prevent malicious software from being loaded on equipment used by the KRO. Only applications required to perform the organization's mission shall be loaded on the computer, and all such software shall be obtained from sources authorized by local policy. Data on the equipment shall be scanned for malicious code on first use and periodically afterward. The equipment shall be located on internal networks behind boundary/perimeter network defenses and afforded protections consistent with Guidance and Policy Memorandum No. 6-8510 "Department of Defense Global Information Grid Information Assurance" for network security at the mission critical level. KRO-related activities shall be performed only on systems approved for use by the KRO's C/S/A.

6.4.4 Anomaly Detection

Key recovery (in particular automated key recovery) must be carried out with extreme caution, as the chance for compromise can be very high. Further, the risk of compromise and the scope of any potential compromise is highly dependent upon the implementation. Therefore, the key recovery infrastructure shall be capable of detecting anomalous key recovery activities and behavior, and reporting them to the PMA and the appropriate C/S/A representative for further action.

6.5 LIFE CYCLE TECHNICAL CONTROLS

Individuals with trusted roles in the key escrow database facility (e.g., system administrators, security officers, operators) shall use security management tools and procedures to ensure that the operational systems and networks adhere to the security requirements. These tools and procedures shall check the integrity of the system data, software, discretionary access controls, audit profile, firmware, and hardware to ensure secure operation.

To ensure that key recovery functions operate with an acceptable level of risk, key escrow databases and KRA workstations must gain approval to operate through a formal accreditation process that satisfies the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) [18].

6.6 NETWORK SECURITY CONTROLS

Network access to Class 3 and Class 4 key escrow databases shall be protected as specified in DoD X.509 CP Section 6.7 for Class 3 and Class 4 CMA equipment. Class 3 and Class 4 key escrow database equipment shall limit services as specified by DoD X.509 CP Section 6.7 for Class 3 and Class 4 CA equipment. Class 4 KRA workstation equipment shall limit services as specified by DoD X.509 CP Section 6.7 for Class 4 RA equipment.

Protection of key escrow database equipment shall be provided against known network attacks as specified by DoD X.509 CP Section 6.7 for CMA equipment. Boundary control devices used to protect the network on which the key escrow database and KRA workstation equipment are hosted shall deny service as specified by DoD X.509 CP Section 6.7 for PKI equipment.

Intrusion detection capabilities for key escrow database equipment and KRA workstations shall be as specified in DoD X.509 CP Section 6.7. Intrusion detection capabilities for Class 3 and Class 4 key escrow databases shall meet the requirements specified by DoD X.509 CP Section 6.7 for Class 3 and Class 4 CA equipment. Intrusion detection capabilities for Class 4 KRA workstation equipment shall meet the requirements specified by DoD X.509 CP Section 6.7 for Class 4 Registration Authority (RA) equipment. Intrusion detection capabilities for Class 3 KRA workstation equipment shall meet the requirements specified by DoD X.509 CP Section 6.7 for Class 3 RA equipment.

6.7 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Requirements for cryptographic modules are stated in section 6.2.1.

7 POLICY ADMINISTRATION

7.1 POLICY CHANGE PROCEDURES

This policy shall be maintained under the specification change procedures identified in DoD X.509 CP Section 8.1.

7.2 PUBLICATION AND NOTIFICATION POLICIES

This policy shall be published as specified in DoD X.509 CP Section 8.2.

7.3 POLICY APPROVAL PROCEDURES

This policy shall be approved based on the procedures specified in DoD X.509 CP Section 8.3.

This page intentionally left blank.

8 REFERENCES

1. ISO/IEC 9594-8/ITU-T Recommendation X.509, "Information Technology – Open Systems Interconnection: The Directory: Authentication Framework," 1997 edition. (Pending publication of 1997 edition, use 1993 edition with the following amendment applied: Final Text of Draft Amendment DAM 1 to ISO/IEC 9594-8 on Certificate Extensions, June 1996.)
2. General Procedures for Registering Computer Security Objects, National Institute for Standards and Technology (NIST) IR 5308, December, 1993.
3. Computer Security Policy, Computer Security Laboratory (CSL) Bulletin CSL94-01, NIST, January, 1994.
4. People: An Important Asset in Computer Security, CSL Bulletin CSL93-10, NIST, October, 1993.
5. Security Engineering Requirements for Cryptographic Modules, NIST, FIPS PUB 140-1, January 1994.
6. Security Engineering Requirements for Cryptographic Modules, NIST, FIPS PUB 140-2, June 2001.
7. Automated Password Generator, Federal Information Processing Standard 181, October, 1993.
8. Minimum Security Requirements for Multi-User Operating Systems, CSL, NISTIR 5153, NIST, March, 1993.
9. Guidance on the Selection of Low Level Assurance Evaluated Products, CSL Bulletin, CSL96-04, NIST, April, 1996.
10. Guideline for Automatic Data Processing Risk Analysis, National Bureau of Standards.
11. Public Key Infrastructure Technical Specification: Part C - Concept of Operations, William E. Burr, NIST.
12. Paulk, Marc, Bill Curtis, Mary Beth Chrissis, and Charles V. Weber, “Capability Maturity Model, Version 1.1,” IEEE Software, Vol. 10, No. 4, July 1993, pp. 18-27.
13. Trusted Software Development methodology, SDI-S-SD-91-000007, June 17, 1992.
14. Common Criteria Implementation Board, *Common Criteria for Information Technology Security Evaluation,* CCIB-98-026, Version 2.1, August 1999.
15. Password Usage, FIPS 112, May 1985.
16. American Bar Association, *Digital Signature Guidelines,* 1996-08-01.
17. ASD(C3I), *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*, DoD Instruction 5200.40, December 30, 1997.
18. X.509 Certificate Policy for the United States Department of Defense, DoD PKI Program Management Office, http://www.c3i.osd.mil/org/sio/ia/pki/documents.html.

19. (Draft) DoD Class 3 Key Recovery Concept of Operations, CygnaCom Solutions, Inc., Version 0.1, 20 March 2000.
20. Requirements for Key Recovery Products: Report of the Technical Advisory Committee (TAC) to Develop a FIPS for the Federal Key Management Infrastructure, Final Report, November 1998.
21. Information Systems Security Policy and Procedures for FORTEZZA® Card Certification Authority Workstation, National Security Agency, Information System Security Office, NAG-69C, February 2000.

9 LIST OF ACRONYMS

CA	Certification Authority
CC	Common Criteria
CM	Certificate Management
CMA	Certificate Management Authority
CP	Certificate Policy
CPS	Certification Practice Statement
C/S/A	Combatant Command, Service, and/or Agency
DISA	Defense Information Systems Agency
DN	Distinguished Name or Directory Name
DoD	Department of Defense
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
FISA	Foreign Intelligence Security Act
I&A	Identification and Authentication
KMI	Key Management Infrastructure
KRA	Key Recovery Agent
KRO	Key Recovery Official
KRP	Key Recovery Policy
KRPS	Key Recovery Practice Statement
NSM	Network Security Manager
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PMO	Program Management Office
TBD	To Be Defined

This page intentionally left blank.

10 GLOSSARY OF TERMS

Encryption Certificate: A certificate containing a public key that is used to encrypt or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. The process of storing, protecting, and escrowing the private component of the key pair associated with the encryption certificate is sometimes referred to as key management.

Key Escrow: The retention of the private component of the key pair associated with a subscriber's encryption certificate to support key recovery.

Key Recovery: Production of a copy of an escrowed key and delivery of that key to an authorized requestor.

Key Recovery Agent (KRA): An individual authorized to interface with the key escrow database in conjunction with one or more other key recovery agents) to cause the key escrow database to carry out key recovery requests, as specified by the Key Recovery Policy.

KRA Workstation: The workstation from which the Key Recovery Agent interfaces with the key escrow database system.

Key Escrow Database: The function, system, or subsystem that maintains the key escrow repository and responds to key registration and key recovery requests from one or more Key Recovery Agents, as specified by the Key Recovery Policy.

Key Recovery Official (KRO): An individual authorized to authenticate and submit key recovery requests to the Key Recovery Agent on behalf of requestors, as specified by the Key Recovery Policy.

Key Recovery Policy (KRP): Specifies the conditions under which key recovery information must be created and conditions under which and to whom escrowed keys may be released; it also indicates who are allowable Key Recovery Agent(s) and Key Recovery Officials and how or where escrowed keys must be maintained.

Key Recovery Practice Statement (KRPS): A Key Recovery Practice Statement is a statement of the practices, procedures, and mechanisms that a key escrow system employs in registering and recovering escrowed keys.

Requestor: An individual who is authorized, under the Key Recovery Policy, to request recovery of a subscriber's escrowed key. Subscribers can always request recovery of their own keys.

Policy Management Authority: Body established to oversee the creation and update of Certificate and Key Recovery Policies, review Certification and Key Recovery Practice Statements, review the results of CA and Key Recovery audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate and Key Recovery policies.

Public Key Infrastructure: Framework established to issue, maintain, and revoke public key certificates.

Security auditor: Local automation security personnel, as required by DoD 5200.28.

Split Key Procedure: A mechanism whereby a key is cryptographically divided into some number of pieces so that when a specific-sized subset of the pieces is recombined the original key can be reconstructed.

Storage Key: The cryptographic key that is used to protect the escrowed keys in the key escrow database.

Subscriber: "An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate." [17] **Current subscribers** possess valid DoD PKI-issued certificates.

Third Party: A person other than the subscriber who requests escrowed keys (e.g., law enforcement, supervisor).

Two person control:
For the purpose of this policy, two person control is a process that requires two independent, authorized parties to consent to activities involving extraction and restoration of private key data.